TROEX Company Data Protection Policy

Context and overview

Key details

- Policy prepared by: Toms Silins
- Approved by board / management on: 22/05/2018
- Policy became operational on: 25/05/2018
- Next review date: 25.05/2019

Introduction

TROEX needs to gather and use certain information about individuals. TROEX is committed to processing data in accordance with its responsibilities under the General Data Protection Regulation (GDPR).

These can include customers, suppliers, business contacts, employees and other people the organization has a relationship with or may need to contact.

This policy describes how this personal data must be collected, handled and stored to meet the company's data protection standards — and to comply with the law.

Why this policy exists

This data protection policy ensures TROEX:

- Complies with GDPR and follows good practice
- Protects the rights of staff, customers and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Data protection principles

The data protection principles describe how TROEX collects, handles and stores personal information. These principles apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the principles, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

There are eight important principles. Personal data must:

- Be processed fairly and lawfully
- Be obtained only for specific, lawful purposes
- Be adequate, relevant and not excessive
- Be accurate and kept up to date
- Not be held for any longer than necessary
- Processed in accordance with the rights of data subjects
- Be protected in appropriate ways
- Not be transferred outside the European Economic Area (EEA), unless that country or territory also ensures an adequate level of protection

Furthermore, Article 5 of the GDPR specifically requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

People, risks and responsibilities

Policy scope

This policy applies to all personal data processed by TROEX.
The Board shall take responsibility for the TROEX ongoing compliance with this policy.
This policy shall be reviewed at least annually.

This policy applies to:

- The head office of TROEX
- All branches of TROEX
- All staff and volunteers of TROEX
- All contractors, suppliers and other people working on behalf of TROEX

It applies to all data that the company holds relating to identifiable individuals. This can include:

- Names of individuals
- Postal addresses
- Email addresses
- Telephone numbers
- …plus any other information relating to individuals

Data protection risks

This policy helps to protect TROEX from some very real data security risks, including:

- **Breaches of confidentiality.** For instance, information being given out inappropriately.
- **Failing to offer choice.** For instance, all individuals should be free to choose how the company uses data relating to them.
- **Reputational damage.** For instance, the company could suffer if hackers successfully gained access to sensitive data.

Responsibilities

Everyone who works for or with TROEX has some responsibility for ensuring data is collected, stored and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

However, these people have key areas of responsibility:

The **Board of Directors** is ultimately responsible for ensuring that TROEX meets its legal obligations.

The **Data Protection Officer** is responsible for:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule.
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy.

- Dealing with requests from individuals to see the data TROEX holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

The **COO** is responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data. For instance, cloud computing services.

The **Marketing Manager** is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

General staff guidelines

The only people able to access data covered by this policy should be those who **need it for their work**.

Data **should not be shared informally**. When access to confidential information is required, employees can request it from their line managers.

TROEX will provide training to all employees to help them understand their responsibilities when handling data.

Employees should keep all data secure, by taking sensible precautions and following the guidelines below.

In particular, **strong passwords must be used** and they should never be shared.

Personal data **should not be disclosed** to unauthorized people, either within the company or externally.

Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of.

Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.

Data storage, lawful, fair and transparent processing

To ensure its processing of data is lawful, fair and transparent, the Charity shall maintain a Register of Systems. The Register of Systems shall be reviewed at least annually. Individuals have the right to access their personal data and any such requests made to TROEX shall be dealt with in a timely manner.

These rules describe how and where data should be safely stored. Questions about storing data safely can be directed to the IT manager or data controller.

When data is **stored on paper,** it should be kept in a secure place where unauthorized people cannot see it.

These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept **in a locked drawer or filing cabinet**.
- Employees should make sure paper and printouts are **not left where unauthorized people could see them**, like on a printer.
- **Data printouts should be shredded** and disposed of securely when no longer required.

When data is **stored electronically**, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:

- Data should be **protected by strong passwords** that are changed regularly and never shared between employees.
- If data is **stored on removable media** (like a CD or DVD), these should be kept locked away securely when not being used.
- Data should only be stored on **designated drives and servers**, and should only be uploaded to an **approved cloud computing services**.
- Servers containing personal data should be **sited in a secure location**, away from general office space.
- Data should be **backed up frequently**. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should **never be saved directly** to laptops or other mobile devices like tablets or smart phones.
- All servers and computers containing data should be protected by **approved security software and a firewall**.

Data use. Lawful purposes. Data minimization.

All data processed by TROEX must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate .

TROEX shall note the appropriate lawful basis in the Register of Systems.

a. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
b. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the TROEX systems.

TROEX shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Personal data is of no value to TROEX unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption or theft:

- When working with personal data, employees should ensure **the screens of their computers are always locked** when left unattended.
- Personal data **should not be shared informally**. In particular, it should never be sent by email, as this form of communication is not secure.
- Data must be **encrypted before being transferred electronically**. The IT manager can explain how to send data to authorized external contacts.
- Personal data should **never be transferred outside of the European Economic Area**.
- Employees **should not save copies of personal data to their own computers.** Always access and update the central copy of any data.

Data accuracy

TROEX shall take reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

The more important it is that the personal data is accurate, the greater the effort TROEX should put into ensuring its accuracy.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.

- Data will be held in **as few places as necessary**. Staff should not create any unnecessary additional data sets.
- Staff should **take every opportunity to ensure data is updated.** For instance, by confirming a customer's details when they call.
- TROEX will make it **easy for data subjects to update the information** TROEX holds about them. For instance, via the company website.
- Data should be **updated as inaccuracies are discovered**. For instance, if a customer can no longer be reached on their stored telephone number, it should be removed from the database.
- It is the marketing manager's responsibility to ensure **marketing databases are checked against industry suppression files** every six months.

Subject access requests

All individuals who are the subject of personal data held by TROEX are entitled to:

- Ask **what information** the company holds about them and why.
- Ask **how to gain access** to it.
- Be informed **how to keep it up to date.**
- Be informed how the company is **meeting its data protection obligations**.

If an individual contacts the company requesting this information, this is called a subject access request.

Subject access requests from individuals should be made by email, addressed to the data controller at customerservice@troex.com. The data controller can supply a standard request form, although individuals do not have to use this.

Individuals will be charged EUR 15 per subject access request. The data controller will aim to provide the relevant data within 14 days.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Disclosing data for other reasons

In certain circumstances, in line with the prevailing legislation, personal data can be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, TROEX will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the board and from the company's legal advisers where necessary.

Archiving and removal.

To ensure that personal data is kept for no longer than necessary, TROEX shall put in place an archiving policy for each area in which personal data is processed and review this process annually.

The archiving policy shall consider what data should/must be retained, for how long, and why.

Security.

TROEX shall ensure that personal data is stored securely using modern software that is kept-up-to-date.

Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information.

When personal data is deleted this should be done safely such that the data is irrecoverable. Appropriate back-up and disaster recovery solutions shall be in place.

Breach.

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, TROEX shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach to the appropriate authorities.